UNIVERSIDAD
DE SANTIAGO
DE CHILE

Facultad de Ciencia

Departamento de Matemática y Ciencia de la Computación

Criptografía I

Laboratorio Nº 2

Nombre:
David Sanhueza Andréus

Profesor:
Rodrigo Abarzúa

Fecha entrega:
miércoles 23 de mayo

Índice

1. Introducción

AES es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica.

El siguiente informe describe la situación de implementar una ronda de la función del AES.

Los datos se obtendrán de manera aleatoria.

Esta función se implementará en lenguaje C.

2. Algoritmos

Para la resolución del problema de implementar la función del AES, se realizaron distinto algoritmos, a continuación se presentan los 2 algoritmos principales:

Algoritmo 1 *GeneradorBit*

Input: A[128]
Output: Arreglo de 128 bits con números binarios

```
1: for i ← 0 to 128 do
2:     A[128] ← rand()
3: end for
```

Algoritmo 2 *ObtenerB*

Input: A[128]
Output: Arreglo B[128]

```
1: for i ← 0 to 128 do
2:     fila ← A[i]*8 + A[i + 1]*4 + A[i + 2]*2 + A[i + 3]*1
3:     columna ← A[i + 4] *8 + A[i + 5]*4 + A[i + 6]*2 + A[i + 7]*1
4:     hexadecimal ← aes_box[fila][columna]
5:     k ← i
6:     for j ← 0 to 4 do
7:         binario1 ← hexadecimalABinario(hexadecimal[0])
8:         binario2 ← hexadecimalAbinario(hexadecimal[1])
9:         B[k] ← binario1[j] - '0'
10:        B[k + 4] ← binario2[j] - '0'
11:        k ← k + 1
12:    end for
13: end for
14: return B[128]
```

3. Formulación del experimento

Para poder obtener los resultados del algoritmo del *AES*, este se implementó en lenguaje *C*, y posteriormente se compiló y ejecutó.

4. Resultados

Dado que el algoritmo es altamente eficiente, el costo en tiempo de este es muy bajo.

El programa fue ejecutado en un computador con las siguientes descripciones:

- Ram: 4 GB
- Procesador: i5 1.6 GHz
- Sistema Operativo: macOS High Sierra 10.13.4

5. Compilación y ejecución de programas

Para poder compilar y ejecutar el programa, se deben ingresar los siguientes comandos:

Compilación

```
gcc lab_2.c -o lab
```

Ejecución

```
./lab
```

6. Conclusiones

Hasta 2005, no se ha encontrado ningún ataque exitoso contra el AES. La Agencia de Seguridad Nacional de los Estados Unidos (NSA) revisó todos los finalistas candidatos al AES, incluyendo el Rijndael, y declaró que todos ellos eran suficientemente seguros para su empleo en información no clasificada del gobierno de los Estados Unidos. En junio de 2003, el gobierno de los Estados Unidos anunció que el AES podía ser usado para información clasificada.